United States District Court
Northern District of California

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

AMY WYNNE,

Plaintiff,

v.

AUDI OF AMERICA, et al.,

Defendants.

Case No. 21-cv-08518-DMR

ORDER DENYING PLAINTIFF'S MOTION TO REMAND

Re: Dkt. No. 19

Plaintiff Amy Wynne filed this putative class action on June 18, 2021 in Marin County Superior Court against Defendant Audi of America alleging claims related to the theft of her personal information resulting from a data breach. She later filed an amended complaint adding Audi of America, LLC; Sanctus LLC dba Shift Digital; Shift Digital, LLC; and Volkswagen Group of America, Inc. ("Volkswagen") as additional Defendants.[1] [Docket No. 1 (Notice of Removal, "NOR") ¶¶ 1-3, Exs. A (Compl.), B (Am. Compl.).] Wynne subsequently dismissed Shift Digital, LLC from the lawsuit. NOR ¶ 2 n.2, Ex. D. Sanctus LLC dba Shift Digital ("Shift Digital") removed the case on November 2, 2021, asserting that federal jurisdiction exists under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d). NOR ¶ 6. Wynne now moves to remand the action. [Docket No. 19.] The court held a hearing on July 14, 2022. For the following reasons, Wynne's motion is denied.

I. BACKGROUND

Wynne makes the following allegations in the amended complaint: Defendant Audi is a wholly-owned subsidiary of Volkswagen. Shift Digital is a vendor that works with Audi and Volkswagen. Am. Compl. ¶¶ 7, 15. Wynne alleges that at some point between August 2019 and

[1] Defendants assert that "Audi of America" and "Audi of America, LLC" are the same entity. NOR ¶ 2 n.1. The court refers to them together in this opinion as "Audi."

May 2021, Defendants were the target of a data breach and her personally identifiable information ("PII") was accessed and compromised. *Id*. at ¶¶ 1, 2, 15-25. The PII included names, home and business addresses, email addresses, driver's license numbers, social security numbers, dates of birth, account and loan numbers, and tax identification numbers. *Id*. at ¶ 18. She alleges that Defendants failed to implement reasonable security procedures to adequately protect her and the putative class members' PII from data breaches, which "resulted in an invasion of her privacy interests." *Id*. at ¶ 6. Further, given the sensitive nature of the information at issue, she and the putative class members are at "imminent, immediate, and continuing risk of further identity theft-related harm." *Id*. at ¶¶ 3, 6, 21, 22.

Wynne defines the putative class as "[a]ll Volkswagen of America, Inc./Audi customers and interested buyers residing in California whose PII was accessed or otherwise compromised in the Data Breach, which, according to the Notice of Data Breach provided by Volkswagen of America, Inc./Audi, occurred at some point between August 2019 and May 2021." *Id*. at ¶ 37. She brings the following claims on behalf of herself and the class: 1) violation of California's Unfair Competition Law ("UCL"), California Business & Professions Code section 17200; and 2) violation of the California Consumer Privacy Act ("CCPA"), California Civil Code section 1798.150 *et seq*.[2] Wynne seeks an award of statutory damages under the CCPA, injunctive and equitable relief, and an award of attorneys' fees and costs. Prayer for Relief.

On November 2, 2021, Shift Digital removed the case under CAFA jurisdiction. Wynne now moves to remand the case to state court, arguing that this court lacks subject matter

---

[2] The CCPA provides in relevant part that

> [a]ny consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action . . .

Cal. Civ. Code § 1798.150(a)(1). The statute authorizes statutory damages, actual damages, injunctive or declaratory relief, and "[a]ny other relief the court deems proper" for violations. Cal. Civ. Code § 1798.150(a)(1)(A)-(C).

jurisdiction because she does not satisfy the requirements of Article III standing.

II. LEGAL STANDARD

Under 28 U.S.C. § 1441(a), a defendant may remove to federal court any matter that originally could have been filed in federal court. *Caterpillar Inc. v. Williams*, 482 U.S. 386, 392 (1987). Federal courts are courts of limited jurisdiction and possess subject matter jurisdiction in civil cases based only on federal question or diversity jurisdiction. *Id.*; *see* 28 U.S.C. §§ 1331, 1332. The removing defendant bears the burden of establishing that removal was proper. *United Computer Sys., Inc. v. AT & T Corp.*, 298 F.3d 756, 763 (9th Cir. 2002). "If at any time before final judgment it appears that the district court lacks subject matter jurisdiction, the case shall be remanded." 28 U.S.C. § 1447(c); *see also Gaus v. Miles, Inc.*, 980 F.2d 564, 566 (9th Cir. 1992) (stating that the removal statute is "strictly construe[d]" and "[f]ederal jurisdiction must be rejected if there is any doubt as to the right of removal in the first instance.").

Article III standing "is a necessary component of subject matter jurisdiction." *In re Palmdale Hills Prop., LLC*, 654 F.3d 868, 873 (9th Cir. 2011). However, "[s]tate courts are not bound by the constraints of Article III," and when federal subject matter jurisdiction is lacking, remand is the correct remedy. *Polo v. Innoventions Int'l, LLC*, 833 F.3d 1193, 1196 (9th Cir. 2016) (citing *ASARCO Inc. v. Kadish*, 490 U.S. 605, 617 (1989)). "The rule that a removed case in which the plaintiff lacks Article III standing must be remanded to state court under § 1447(c) applies as well to a case removed pursuant to CAFA as to any other type of removed case." *Id.* (citations omitted).

III. DISCUSSION

Wynne argues that the case must be remanded because the court lacks subject matter jurisdiction. Specifically, Wynne argues that she has not alleged a "concrete" harm necessary to confer Article III standing under *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2200 (2021).

Article III standing requires three elements: "[t]he plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016) (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992)). As the removing

party asserting federal jurisdiction, Shift Digital bears the burden of establishing these elements. *Lujan*, 504 U.S. at 561. "To establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Spokeo*, 578 U.S. at 339 (citing *Lujan*, 504 U.S. at 560). While a concrete injury need not be tangible, "it must actually exist"; that is, it must be "real, and not abstract." *Id*. at 340 (quotation marks and citation omitted).

The parties dispute whether Wynne has alleged a "concrete" injury in fact; causation and redressability are not at issue.

Recent Supreme Court decisions have clarified what constitutes a "concrete" injury for purposes of Article III standing. In *Spokeo*, the Court held that "Article III standing requires a concrete injury even in the context of a statutory violation"; an allegation of "a bare procedural violation, divorced from any concrete harm," does not satisfy the injury in fact requirement of Article III. 578 U.S. at 341.

In *TransUnion*, the Court examined "[w]hat makes a harm concrete for purposes of Article III[.]" 141 S. Ct. at 2204. The class action plaintiffs in *TransUnion* sued a credit reporting agency under the Fair Credit Reporting Act ("FCRA"), alleging that the agency "failed to use reasonable procedures to ensure the accuracy of their credit files, as maintained internally by TransUnion." *Id*. at 2200. TransUnion provided misleading credit reports to third-party businesses for 1,853 class members; specifically, it disseminated credit reports containing the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC") alerts that labeled the class members as potential terrorists, drug traffickers, or serious criminals. *Id*. at 2200, 2209. The remaining 6,332 class members had misleading OFAC alerts in their credit files, but the parties stipulated that TransUnion did not provide those plaintiffs' credit information to any potential creditors during the class period. *Id*. at 2209.

In order to determine whether a harm is sufficiently concrete to confer Article III standing, the Court instructed trial courts to "assess whether the alleged injury to the plaintiff has a 'close relationship' to a harm 'traditionally' recognized as providing a basis for a lawsuit in American courts," and "ask[ ] whether plaintiffs have identified a close historical or common-law analogue

for their asserted injury." *Id.* Noting that "traditional tangible harms, such as physical harms and monetary harms" "readily qualify as concrete injuries under Article III," the Court observed that "intangible harms can also be concrete," including "reputational harms, disclosure of private information, and intrusion upon seclusion." *Id.* (citations omitted). Further, while holding that "Congress's views may be 'instructive'" in determining whether a harm is sufficiently concrete, the Court explained that "Congress's creation of a statutory prohibition or obligation and a cause of action does not relieve courts of their responsibility to independently decide whether a plaintiff has suffered a concrete harm under Article III . . ." *Id.* at 2204-05. The Court emphasized that "[o]nly those plaintiffs who have been *concretely harmed* by a defendant's statutory violation may sue that private defendant over that violation in federal court." *Id.* at 2205 (emphasis in original). "An injury in law is not an injury in fact." *Id.*

Applying those principles to the class members' claims, the Court concluded that the 1,853 plaintiffs whose credit reports were provided to third party businesses suffered a concrete injury in fact under Article III. The Court reasoned that this group of class members "suffered a harm with a 'close relationship' to the harm associated with the tort of defamation." *Id.* at 2208-09. The Court reached a different conclusion as to the 6,332 remaining class members, finding that they had suffered no concrete harm since their credit reports were not sent to any third parties: "[t]he mere presence of an inaccuracy in an internal credit file, if it is not disclosed to a third party, causes no concrete harm." *Id.* at 2209-10. The Court emphasized that there was "no historical or common-law analog" to the alleged FCRA violation "where the mere existence of inaccurate information, absent dissemination, amounts to concrete injury." *Id.* at 2209.

The Court also rejected the argument that the 6,332 class members suffered a concrete harm "based on an asserted *risk of future harm*," that is, the risk that the information in the credit reports "would be disseminated in the future to third parties and thereby cause them harm." *Id.* at 2210 (emphasis in original). The Court found persuasive TransUnion's argument "that in a suit for damages, the mere risk of future harm, standing alone, cannot qualify as a concrete harm—at least unless the exposure to the risk of future harm itself causes a *separate* concrete harm." *Id.* at 2210-11 (emphasis in original); *see also id.* at 2213 (holding that "the risk of future harm on its

own does not support Article III standing for the plaintiffs' damages claim"). According to the Court, the 6,332 class members had not demonstrated "that the risk of future harm materialized" in the form of dissemination of the inaccurate OFAC alerts or the denial of credit, or "that they had suffered some other injury (such as an emotional injury) from the mere risk that their credit reports would be provided to third-party businesses." *Id*. at 2211. The alleged risk of future harm "was too speculative to support Article III standing" since the class members did not demonstrate a "sufficient likelihood" that either their credit information would be requested by third parties and provided by TransUnion during the relevant time period, or that TransUnion would intentionally or accidentally release the information to third parties. *Id*. at 2212.

In sum, under *Spokeo* and *TransUnion*, neither "the risk of future harm, without more," nor "bare procedural violation[s], divorced from any concrete harm," suffice for Article III standing in a suit for damages. *Id*. at 2211, 2213 (alteration in original) (quoting *Spokeo*, 578 U.S. at 341).

Shift Digital argues that Wynne has alleged several concrete injuries that give rise to Article III standing. First, it argues that "[a] CCPA plaintiff may sue only when her personal information becomes subject to 'an unauthorized access' and then is exfiltrated, stolen, or disclosed because of inadequate security." Opp'n 4 (citing Cal. Civ. Code § 1798.150(a)(1)). Therefore, it contends, "[b]ecause [section 1798.150(a)(1)] vindicates a substantive privacy right, the alleged violation of that provision gives rise to Article III standing, even without any further harm." Opp'n 4. It also asserts that Wynne has alleged injuries in the form of an increased risk of identity theft or fraud and the expense of credit-monitoring services. *Id*. at 8.

To the extent that Shift Digital contends that an alleged violation of the CCPA alone is sufficient to confer standing, *TransUnion* expressly rejected such an argument, holding that "[u]nder Article III, an injury in law is not an injury in fact. Only those plaintiffs who have been concretely harmed by a defendant's statutory violation may sue that private defendant over that violation in federal court." *TransUnion*, 141 S. Ct. at 2205. However, the injury that gives rise to the alleged violation of the CCPA—that is, the "invasion of [Wynne's] privacy interests" that occurred as a result of the theft of her PII, is a concrete injury that establishes Article III standing. *See* Am. Compl. ¶ 6. As noted, the Supreme Court instructed in *TransUnion* that "courts should

assess whether the alleged injury to the plaintiff has a 'close relationship' to a harm 'traditionally recognized as providing a basis for a lawsuit in American courts," and noted that "disclosure of private information" is an intangible harm that is "traditionally recognized as providing a basis for lawsuits in American courts." *TransUnion*, 141 S. Ct. at 2204. This is consistent with longstanding Ninth Circuit precedent recognizing that historical privacy rights "'encompass[ ] the individual's control of information concerning his or her person' . . . the violation of which gives rise to a concrete injury sufficient to confer standing." *See In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 598 (9th Cir. 2020) (quoting *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017)). For example, in *In re Facebook*, the Ninth Circuit held that plaintiffs had standing to bring privacy-related claims under the Wiretap Act, Stored Communications Act, and California Invasion of Privacy Act based on Facebook's collection of personal information that provided "a cradle-to-grave profile without users' consent." *Id*. at 598-99. The Ninth Circuit concluded that the plaintiffs had "adequately alleged that Facebook's tracking and collection practices would cause harm or a material risk of harm to their interest in controlling their personal information." *Id*. at 599.

In this case, Wynne alleges that sensitive personal information, including names, addresses, driver's license numbers, social security numbers, dates of birth, account and loan numbers, and tax identification numbers, were stolen in a massive data breach. *See* Am. Compl. ¶¶ 2, 18. According to Wynne, the data breach that resulted in the disclosure of Wynne's and the putative class members' PII violated their "fundamental privacy rights." *Id*. at ¶ 3. Under *TransUnion* and Ninth Circuit precedent, these allegations establish an injury that is sufficiently concrete for purposes of Article III standing. *See, e.g., Al-Ahmed v. Twitter, Inc.*, No. 21-cv-08017-EMC, 2022 WL 1605673, at *7-8 (N.D. Cal. May 20, 2022) (holding that "invasion of privacy" resulting from Twitter employees' unauthorized access of Twitter accounts containing private information "is a particularized injury sufficient to establish Article III standing"). The court thus has subject matter jurisdiction over this action.[3]

[3] After the hearing, Plaintiff identified *I.C. v. Zynga, Inc.*, No. 20-cv-01539-YGR, 2022 WL 2252636 (N.D. Cal. Apr. 29, 2022), in a Statement of Recent Decision. [Docket No. 57.] As an

At the hearing, Wynne's counsel argued that Wynne has not alleged a concrete injury for purposes of Article III standing because she only seeks statutory damages for Defendants' "violation of the duty to implement and maintain reasonable security procedures and practices . . . to protect the personal information" that was accessed in the data breach. *See* Cal. Civ. Code § 1798.150(a)(1) (authorizing damages of up to $750 per consumer per incident). Although it is true that the CCPA provides a private right of action that is tied to a defendant's failure to protect California residents' personal information, counsel's argument ignores that such an action may only be brought upon the "unauthorized access and exfiltration, theft, or disclosure" of the individual's information. In other words, a defendant's failure "to provide reasonable security" for personal information is actionable only in the event that the private information is disclosed, resulting in an individual's loss of "control over their personal information" and violation of their right to privacy. *See Eichenberger*, 876 F.3d at 983. The violation of Wynne and the putative class members' right to privacy is precisely what is at issue in this action.

As noted, Shift Digital also argues that Wynne has alleged concrete harms in the form of

---

initial matter, Plaintiff's filing does not comply with Civil Local Rule 7-3(d)(2), which provides that "[b]efore the noticed hearing date, counsel may bring to the Court's attention a relevant judicial opinion published after the date the opposition or reply was filed by filing and serving a Statement of Recent Decision." Plaintiff filed her Statement of Recent Decision on July 19, 2022, five days *after* the July 14, 2022 hearing, and the opinion was dated April 29, 2022, over a month *before* Plaintiff filed her reply brief.

In any event, *Zynga* does not change the outcome of this decision. In *Zynga*, a group of individual gamers sued a game developer following a data breach that resulted in the theft of email addresses, phone numbers, and online usernames. 2022 WL 2252636 at *2, 7. In relevant part, the Honorable Yvonne Gonzalez Rogers held that the plaintiffs had not alleged a concrete injury on the ground that "the type of harm they suffered as a result of the data breach is not analogous to the type of harm suffered as a result of [the theft of] private information." The court noted that it was "hard pressed to conclude that basic contact information, including one's email address, phone number, or Facebook or Zynga username, is private information. All of this information is designed to be exchanged to facilitate communication and is thus available through ordinary inquiry and observation." *Id*. at *7-8. The hackers also stole one plaintiff's date of birth and three plaintiffs' gaming account passwords. The court found that the date of birth was a matter of public record, and that it was not clear how discovery of the passwords "would be 'highly offensive to a reasonable person,' particularly where there [was] no allegation that the gaming accounts . . . contain confidential information." *Id*. at *8. Accordingly, the court concluded "that the privacy injuries alleged . . . are not sufficiently concrete to provide the basis for Article III standing." *Id*. In contrast, the PII at issue in this case includes highly sensitive information, including driver's license numbers, social security numbers, and account and loan numbers, none of which are matters of public record or readily observable.

an increased risk of identity theft or fraud and the expense of credit-monitoring services. Opp'n 8. Since the court concludes that the disclosure of Wynne's sensitive personal information violated her right to privacy and constitutes a concrete harm, it need not address whether these additional injuries are concrete for purposes of Article III.

IV. CONCLUSION

For the foregoing reasons, the court concludes that Wynne has alleged a concrete injury under Article III. Accordingly, as the court has subject matter jurisdiction over this action, it denies Wynne's motion to remand.

IT IS SO ORDERED.

Dated: July 25, 2022

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
IT IS SO ORDERED
Judge Donna M. Ryu

Donna M. Ryu
United States Magistrate Judge